

SIGNATURE EXTRACTION SYSTEM AND METHOD

Peter Szor

ABSTRACT

Host computer systems automatically detect malicious
5 code. The host computer systems automatically generate and
send malicious code packets of the malicious code to a local
analysis center (LAC) computer system. Based on the received
malicious code packets, the LAC computer system provides a
signature update to a network intrusion detection system.
10 Further, the LAC computer system also automatically sends
malicious code signatures of the malicious code to a global
analysis center. In this manner, the spread of the malicious
code is rapidly detected and prevented.